MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2017/2018

TSN3251 / TSC2211 – COMPUTER SECURITY

(All sections / Groups)

14 OCTOBER 2017
2.30 p.m - 4.30 p.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of **NINE pages (excluding this page)** with **FIVE questions.**

2. Answer all **FIVE** questions. Each question carries **20 marks** and the distribution of the marks for each subdivision is given. Maximum allotted are **100 marks**.

3. Please write all your answers in the Answer Booklet provided.

*Answer all **FIVE** questions. Each question carries 20 marks and the distribution of the marks for each subdivision is given.* ***(5×20=100 marks)***

QUESTION 1:

a. State and briefly explain the THREE key objectives at the heart of computer security, which is known as **CIA triad,** with an example each.
(3×2=6 marks)

b. (i) State any TWO differences between **passive and active security attacks.**
(2 marks)

(ii) List any TWO categories each of passive and active security attacks.
(2 marks)

(iii) Identify the **type of security attack** in the following example and explain briefly. **(2 marks)**

"Thousands of e-mails have been sent continuously to a server every day using a phony return e-mail address."

c. Briefly explain what is meant by **'Chosen-plaintext' cryptanalytic attack**.
(2 marks)

d. Draw the basic model for **symmetric** cryptosystem to provide **confidentiality**.
(4 marks)

e. Answer the following with respect to a cricket team consisting of 11 players and a coach. Assume the **usage of symmetric cryptosystem**. **(2 marks)**

(i) Identify the number of secret keys needed if all the players in the team wish to send secret messages to each other.

(ii) Identify the number of secret keys needed in a scheme, where the coach of the team is trusted authority and if a player wishes to send a message to another player, he/she should send it to the coach and the coach sends the message to the other player.

Continued...

QUESTION 2:

a. Assume that plaintext and ciphertext characters are represented as numerical values in Z_{26} as follows:

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Assume the usage of **Affine Cipher**. Decrypt the following ciphertext with $\mathbf{k_1=7}$ and $\mathbf{k_2=6}$ in **modulus 26**, where the key k_1 is used with multiplicative cipher and the key k_2 is used with additive cipher.

Given Ciphertext: **RAN**

(4 marks)

c. (i) Construct a **Playfair matrix** with the key *inspiration*. **(2 marks)**

(ii) Using the constructed Playfair matrix, encrypt the following message.

unknown is an ocean **(4 marks)**

d. The encryption key in a **single stage keyed block/columnar transposition cipher** is given as follows:

3 1 4 2

(i) Identify the **decryption key.**

(ii) **Decrypt** the following ciphertext using the above cipher and key.
(Note: Steps involved: (i) Write column by column (ii) Decrypt using decryption key (iii) Read row by row)

OTOEX TGSTC UITAX HHNHT

Note: Assume that x is the filler character.

(1+3=4 marks)

Continued...

e. One of the criteria for S-box design in **Data Encryption Standard (DES)** is given below:

> **"If we change a single bit in the input to an S-box, two or more bits will be changed in the output"**

Prove the above criteria by applying the pair of inputs, **101101** and **001101** individually to S-box 1 and obtaining their outputs.

Definition of S-box 1

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

(4 marks)

f. With reference to **Double Data Encryption Standard (DES)**, briefly explain **meet-in-the middle** (know plaintext) **attack**.

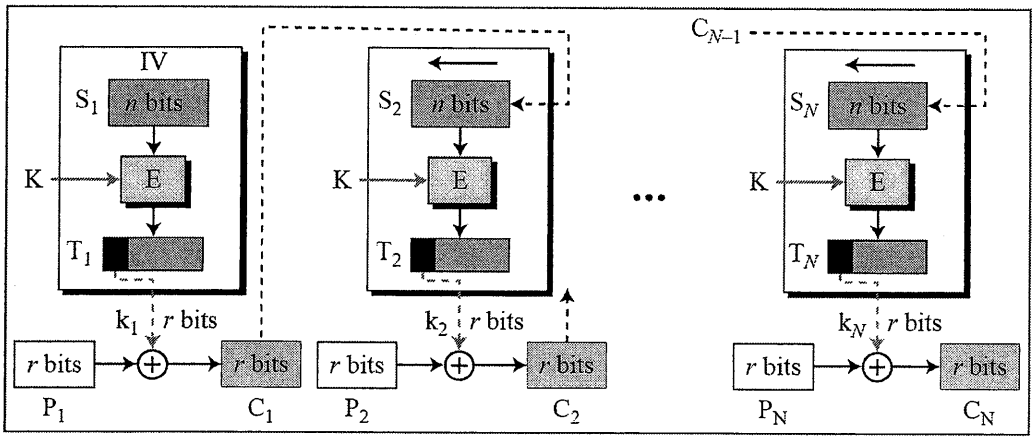
(2 marks)

Continued...

QUESTION 3:

a. With reference to the following diagram that shows the encryption process for **Cipher Feedback (CFB) mode** to be used with modern block ciphers for enciphering text of any size, answer the following:

E : Encryption D : Decryption S_i: Shift register
P_i: Plaintext block i C_i: Ciphertext block i T_i: Temporary register
K: Secret key IV: Initial vector (S_1)



Encryption

(i) Briefly explain the **encryption process** with the help of the above diagram. **(3 marks)**

(ii) Modify the above diagram to show **decryption process**. **(2 marks)**

b. With reference to **Advanced Encryption Standard (AES)**, answer the following:

(i) Given the plaintext
(33 44 55 66 FF EE DD CC BB AA 77 88 99 00 11 $22)_H$
show the **original contents** of **State**, displayed as a 4×4 matrix.
(2 mark)

(ii) If ***a*** and ***b*** are two bytes, prove the nonlinearity of the **SubBytes transformation** by performing the following operation.

SubBytes $(a \oplus b) \neq$ **SubBytes** $(a) \oplus$ **SubBytes** (b)

Use SubBytes Transformation table given and the values
$a = (0011\ 0110)_2$ *and* $b = (1001\ 1100)_2$ **(2 marks)**

Continued...

Note:

Substitute Bytes Transformation Table (AES S-Boxes)

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*A*	*B*	*C*	*D*	*E*	*F*
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*A*	*B*	*C*	*D*	*E*	*F*
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	CB	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(iii) Assume that state before performing ShiftRows transformation on a specific round for **AES** is given below.

$$State(beforeShiftRows) = \begin{bmatrix} FF & EE & DD & CC \\ 00 & 11 & 22 & 33 \\ BB & AA & 99 & 88 \\ 44 & 55 & 66 & 77 \end{bmatrix}$$

Identify the **state after performing ShiftRows transformation.** **(2 marks)**

Continued...

c. With reference to **Rivest-Shamir-Adleman (RSA)** cryptosystem, answer the following:

(i) Identify the **public key {e,n} and private key {d,n}** for the following data using RSA_Key_Generation algorithm given below. **(4 marks)**

p=17; q=31; e=7

where
p and q are two prime numbers
e is an integer with gcd (ϕ (n) , e) =1; 1 < e < ϕ (n);

```
RSA_Key_Generation
{
    Select two large primes p and q such that p ≠ q.
    n ← p × q
    φ(n) ← (p − 1) × (q − 1)
    Select e such that 1 < e < φ(n) and e is coprime to φ(n)
    d ← e^-1 mod φ(n)                    // d is inverse of e modulo φ(n)
    Public_key ← (e, n)                  // To be announced publicly
    Private_key ← d                      // To be kept secret
    return Public_key and Private_key
}
```

(ii) With the help of the following algorithm, perform **encryption** using the keys derived in (i) and using the plaintext message **P=2.** **(2 marks)**

```
RSA_Encryption (P, e, n)                 // P is the plaintext in Z_n and P < n
{
    C ← Fast_Exponentiation (P, e, n)    // Calculation of (P^e mod n)
    return C
}
```

d. With reference to **inv-knapsackSum** algorithm given below, find the elements of 'a', which are to be dropped in the knapsack for the following data:
Predefined tuple: a = [10 17 33 65 135 275 550 1100];
Sum of elements in the knapsack, s=600.

(3 marks)

```
inv_knapsackSum (s, a[1 ... k])
{
    for (i = k down to 1)
    {
        if s ≥ a_i
        {
            x_i ← 1
            s ← s − a_i
        }
        else x_i ← 0
    }
    return x[1 ... k]
}
```

Continued...

QUESTION 4:

a. Give an example for the **type of malware** which
   (i) Requires a host program (ii) does not require a host program
   (iii) Can replicate (iv) does not replicate
   (4 marks)

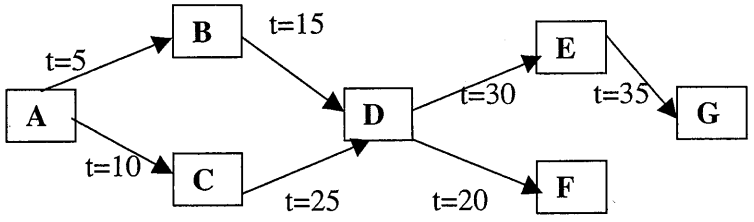
b. State what is meant by **'Trojan Horse'** and **'Trapdoor'**.
   (2 marks)

c. Identify the **type of attack** used in the following situation and briefly explain your answer. **(4 marks)**

   (i) A programmer for a bank is transferring 1 Sen of the monthly interest calculation on each bank customer's account to his own account through a code written as part of the interest calculation program. Assume that if the bank has 1,000,000 customers, the programmer would be able to get RM 10,000 every month in his account.

   (ii) A student has got a computer game which he/she plays at home. Whenever his/her parent checks, the student hits SHIFT-S on his keyboard and it pops up an image of a study material on the screen.

d. With reference to database access control, assume that the convention followed for **cascading authorization** is given below:
   The grant option is used to enable an access right to cascade through a number of users. If a user has an access right with grant option, the user may pass the right to another user. When user **'S'** revokes an access right, any cascaded access right is also revoked, unless that access right would exist even if the original grant from **'S'** had never occurred. Time of grant is also considered for revoking the access right.
   Answer the following question based on the above convention:
   Show the resulting **diagram of access right dependencies** if the user **'B'** revokes the access right to **'D'** at **t=40** and briefly **explain** your answer. **(4 marks)**



e. State what is meant by **SQL injection (SQLi) attack** and give a typical **example.**
   (4 marks)

f. State what you mean by **"inference attack"** in relation to database security.
   (2 marks)

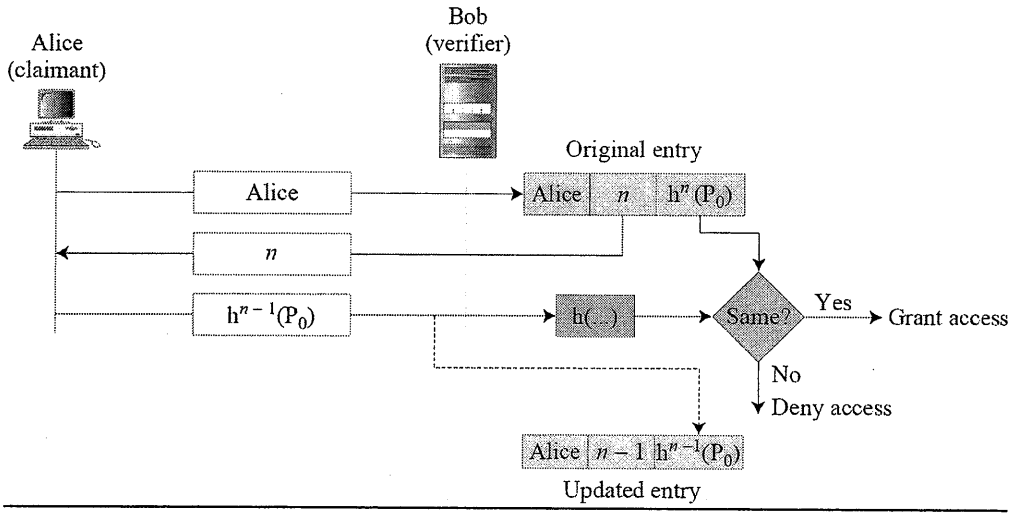
Continued...

QUESTION 5:

a. State and briefly explain the FOUR basic steps that should be used to **secure an operating system**. **(2 marks)**

b. Briefly explain what do you mean by '**reference monitor**' with respect to operating system security. **(2 marks)**

c. The approach devised by Leslie Lamport for **one time password authentication** is shown in the diagram below. Briefly explain the steps involved in this approach. **(4 marks)**



d. State any two physiological and two behavioral traits that can be used for **biometric authentication**. **(2 marks)**

e. Briefly explain the following types of **network security threats**. **(4 marks)**

(i) IP address spoofing

(ii) Phishing

Continued...

f. (i) State the main difference between **Stateless and Stateful Firewalls.** **(2 marks)**

(ii) The **black list** and the **white list** approaches are the two fundamental approaches to create **firewall policies** to effectively minimize vulnerability to the outside world while maintaining the desired functionality for the machines in the trusted internal network. State the major difference between these two approaches. **(2 marks)**

g. State any FOUR major issues to be addressed by a **security plan.** **(2 marks)**

END OF EXAM